AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Dropbox account dblouin1966@gmail.com

Case No. MJ16-490

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
The Dropbox account as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Nothern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252 (a)(2)	Receipt and distribution of child pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[signature]
Applicant's signature

TOBY LEDGERWOOD, SPECIAL AGENT DHS/HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11-21-16

[signature]
Judge's signature

City and state: Bellingham, Washingon

PAULA L. MCCANDLIS, U.S. MAGISTRATE JUDGE
Printed name and title

2016R01225

ATTACHMENT A

Place to be Searched

All information associated with the Dropbox account "dblouin1966@gmail.com" stored at premises owned, maintained, controlled, or operated by Dropbox, a company headquartered at 185 Berry Street, Suite 400, San Francisco, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Section I - Items to be to be Provided by Dropbox Inc. for Search

1. All electronically stored information and communications contained in the Dropbox account, "dblouin1966@gmail.com" including associated email addresses; alternate email addresses; associated cloud storage; account registration information, user contact information, linked web addresses and posted images, content and logs; including a copy of these accounts.

2. All subscriber records associated with the specified accounts, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

3. Log records, including IP address captures, associated with the specified accounts;

4. Any address lists or buddy/contact lists associated with the specified account(s); and

5. Any records of communications between Dropbox Inc., and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified accounts. This is to include records of contacts between the subscribers and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Section II - Items to be Seized

From all electronically stored information and communications contained in the Dropbox account "dblouin@gmail.com" including associated email addresses; alternate email addresses; associated cloud storage accounts to include contents of electronic files:

a. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the accounts specified, or who exercise in any way any dominion or control over the specified accounts;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Any address lists or buddy/contact lists associated with the specified accounts;

c. All images of child pornography and any messages, documents and profile information, attachments, or other data related to child pornography or the possession, receipt, or distribution of child pornography;

d. All subscriber records associated with the specified accounts, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number(s);

e. Any and all other log records, including IP address captures, associated with the specified accounts; and

f. Any records of communications between Dropbox Inc. and any person about issues relating to the specified accounts, such as technical problems, billing inquiries, or complaints from other users about the specified accounts. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF WHATCOM)

I, Toby Ledgerwood, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent since 2006. Prior to this assignment, I worked as a United States Customs Inspector from 2002 to 2006. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2013, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have observed and reviewed thousands of examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of many search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. Further, I have served as the affiant on numerous search warrants and complaints relating to child exploitation investigations. I am a member of the Internet

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. I have attended periodic seminars, meetings, and training. I attended the ICAC Undercover Investigations Training Program in Alexandria, Virginia, in June 2014 regarding child exploitation. I also attended the Crimes Against Children Conference in Dallas, Texas, in August 2014, where I received training relating to child exploitation, including training in the Ares Peer to Peer (P2P) file sharing program. In September 2015, I received training in the Emule (P2P) file sharing program. I received a Bachelor of Science degree in Criminal Justice with a minor in Sociology from the University of Missouri-St. Louis.

2. I make this Affidavit in support of an application, pursuant to 18 U.S.C. § 2703, for a warrant to search any and all information for Dropbox Inc. account "dblouin1966@gmail.com" (hereinafter the SUBJECT ACCOUNT), to include any and all associated cloud storage accounts and their contents, including without limitation any electronic files that the subscriber has stored in the accounts. The SUBJECT ACCOUNT is controlled by Dropbox Inc. (hereinafter referred to as "Dropbox"). This application seeks a warrant to search the SUBJECT ACCOUNT and seize the items listed in Attachment B, which is attached to this Affidavit and incorporated herein by reference, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found in the SUBJECT ACCOUNT.

II. BACKGROUND REGARDING DROPBOX

5. In my training and experience, I have learned that Dropbox was founded in 2007 and is a privately held electronic file storage service headquartered in San Francisco, California. Dropbox is a file hosting service that allows users to upload and sync files to cloud storage and then access them from a web browser or app on their computer or digital device. It is a simple online virtual storage utility that allows users to make their files accessible from almost anywhere. Dropbox allows users to keep the files private, share them with contacts, or make the files public. Dropbox also allows users to create a special folder or link on their computers or digital devices, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer or device is used to access it. Files placed in this folder are also accessible via the Dropbox website and mobile apps. Dropbox users can also share files or folders they create with other Dropbox users. Dropbox provides both free and fee-based file sharing and file synchronization services. Dropbox stores files in user accounts until the user deletes them. Dropbox saves deleted files for 30 days. If a Dropbox account is deleted, the files and account information will be purged after 30 days.

6. Dropbox users create Dropbox accounts, which are identified by the user's e-mail address and secured with a user password. The e-mail address is the unique identifier for a Dropbox account. Once an account is created with Dropbox, the user must enter his or her e-mail address for the account along with a valid user-created password in the login screen in order to access the account. Since Dropbox accounts are not

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

publicized and the general login screen does not show other valid e-mail accounts, the user must know the e-mail address in the first step to access a Dropbox account.

7. Cloud storage providers like Dropbox typically retain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Dropbox's website or application), and other log files that reflect usage of the account. In addition, cloud storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the cloud storage account, which can help establish the individual or individuals who had dominion and control over the account.

8. Dropbox conducts business throughout the United States and the world through its file-sharing services.

9. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in child pornography:

a. Those who receive and attempt to receive child pornography over the Internet often maintain their collections which are in a digital or electronic format in a safe, secure and private environment, such as a computer or cloud storage service. These collections are often maintained for several years and are kept where the individual can easily access them, such as at the individual's residence or on a digital or electronic storage device.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

c. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

d. In the case of those who receive and attempt to receive child pornography via email, the nature of email itself provides a convenient means by which these individuals can access their collections from any computer, at any location with Internet access. These individuals therefore do not need to physically carry their collections with them, but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

III. STATEMENT OF PROBABLE CAUSE

10. Between April 08, 2016, and April 09, 2016, while acting in an undercover capacity, I used a law enforcement version of eMule, a commonly used P2P file sharing program for the eD2k file sharing network, to monitor for P2P users possessing and distributing image and video files depicting child pornography. I used the law enforcement version of eMule to download several files depicting child pornography from a P2P user at IP address 50.135.153.216 (the SUBJECT IP ADDRESS). Two of the undercover downloads are detailed below.

11. On April 09, 2016, between approximately 0537 (UTC) and 0610 (UTC), I used the law enforcement version of eMule to establish a single-source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

suspected child pornography video file entitled "[Boy+Man] – Man Fucks Pub Boy and 12yo Brother.mpg" (hereinafter the "subject video file #1"). The law enforcement version of eMule initiated a download of the subject video file #1 and successfully downloaded a partial file (4 minute and 30 second video) from the user at the SUBJECT IP ADDRESS.

12. I have observed the subject video file #1. Based on my training and experience, the file meets the federal definition of child pornography, as defined in 18 U.S.C. § 2256(8), as it depicts lascivious exhibition of the genitals or pubic areas of a minor child, and/or a minor child engaged in sexually explicit conduct. I have described the subject video file below:

> **Filename: [Boy+Man] – Man Fucks Pub Boy and 12yo Brother.mpg**
> This color video, approximately 4 minutes and 30 seconds in length, depicts a prepubescent male (hereinafter the "child victim") being sexually abused by an adult male. The child victim is fully visible in the video. The child victim is nude and laying on his back during the initial part of the encounter. The child victim's unclothed genital area is the focal point of the video. A hairy, adult male inserts his erect penis into the child victim's anus and performs sexual intercourse. The child victim has no visible pubic hair and is small in stature as compared to the adult male. The child victim lacks muscular development. The child victim appears to be approximately 8 to 10 years old.

13. On April 09, 2016, between approximately 1600 (UTC) and 1602 (UTC), I used the law enforcement version of eMule to establish a single source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of a suspected child pornography video file entitled "Gerbys Ii013-Preteen Boy-Pedo Gay Boy Cum.mpg" (hereinafter the "subject video file #2"). The law enforcement version of eMule initiated a download of the subject video file #2 and successfully downloaded a partial file (3 minute 45 second video) from the user at the SUBJECT IP ADDRESS.

14. I have observed the subject video file #2. Based on my training and experience, the file meets the federal definition of child pornography, as defined in 18 U.S.C. § 2256(8), as it depicts lascivious exhibition of the genitals or pubic areas of a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

minor child, and/or a minor child engaged in sexually explicit conduct. I have described the subject video file #2 below:

> **Filename: Gerbys Ii013-Preteen Boy-Pedo Gay Boy Cum.mpg**
> This color video, approximately 3 minutes and 45 seconds in length, depicts a minor male (hereinafter the "child victim"). At the beginning of the video, the child victim is clothed and observed undressing. The child victim then proceeds to take off all his clothing and the unclothed genital area is the main focal point of the video, as the camera zooms into the child victim's genital area on multiple occasions. The child victim proceeds to masturbate continuously throughout the video. The child victim has no visible pubic hair and is young in appearance and lacking muscular development. The child victim is approximately 11 to 13 years old.

15. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to ISP Comcast Communications.

16. On September 22, 2016, a Department of Homeland Security (DHS) administrative summons' was submitted to Comcast requesting subscriber information for the SUBJECT IP ADDRESS during the date and time the subject video files were downloaded.

17. On September 23, 2016, Comcast provided the requested information. During the dates and times the subject video files were downloaded, the SUBJECT IP ADDRESS was assigned to Douglas BLOUIN at the residence located at 9936 Collins Rd, Sedro Woolley, Washington (the SUBJECT PREMISES). Comcast revealed the IP History of the SUBJECT IP ADDRESS to have a lease grant date and time of March 27, 2016, at 17:20:55 UTC and a lease expiration of September 22, 2016, at 00:00:00 UTC. The SUBJECT IP ADDRESS is leased to Douglas BLOUIN with account number ending in 0849.

18. On September 26, 2016, I conducted a criminal history search of BLOUIN. The search revealed BLOUIN has previous convictions in Skamania County for two counts of Child Molestation 1. BLOUIN is a registered sex offender, and his sex offender registration record reflects that BLOUIN is registered at the SUBJECT PREMISES and has been since August 31, 2004.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. On October 27, 2016, HSI Agents conducted a search warrant at the SUBJECT PREMISES. At approximately 7:44 a.m., SA Ledgerwood introduced himself and SA Smith to BLOUIN. SA Ledgerwood asked BLOUIN if agents could record the interview and BLOUN stated yes. SA Ledgerwood informed BLOUIN that he was not under arrest, and BLOUIN was not place in restraints during the interview. SA Ledgerwood read BLOUIN his rights per Miranda with SA Smith witnessing. BLOUIN indicated he understood his rights and was willing to speak with agents.

20. Among other things, BLOUIN stated the primary computer he used was the Dell 660 that was located in his home office. BLOUIN stated his wife never used that computer. BLOUIN confirmed that he used P2P filesharing programs to obtain and view child pornography and that he had been doing so for some time. He stated that he generally viewed images and videos of boys between 7 and 14 years old. He told me that it was unlikely that any child pornography would be found on any of his devices because he regularly wiped his hard drive. A forensic examination of his Dell computer revealed the process of P2P filesharing applications, including the application from which the videos described above were downloaded, and the wiping software BLOUIN reported using to wipe his hard drive.

21. BLOUIN stated he had never sent or received child pornography using email accounts. Asked about his activity on the internet, BLOUIN said that he had previously used Google to search for child pornography. BLOUIN also described a website he used to access child pornography. BLOUIN stated a subject posts links that take users to child pornography in "yandex or dropbox." BLOUIN stated the site was "loaded."

22. SA Ledgerwood asked if BLOUIN if he remembered when the last time he was sharing or downloading child pornography, and he stated he did not know. BLOUIN later acknowledged it could have been as recently as within the last week. SA Ledgerwood asked if he was doing this a lot in April of 2016, and BLOUIN stated it was a good possibility. SA Ledgerwood asked BLOUIN if he recognized the names of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

child pornography video files that Agents downloaded. BLOUIN stated he did not recognize the first file name but the second video file name that contained the work "Gerbys" looked familiar.

23. Among the items found on BLOUIN's home was a green notebook recovered from his home office. I examined this notebook and found a reference to a Dropbox account under the user name dblouin1966@gmail.com. During his interview, BLOUIN stated that he had an email address with the same username.

24. BLOUIN was arrested the same day as the execution of the search warrant, and the grand jury has since returned an indictment charging BLOUIN with one count each of receipt and possession of child pornography.

IV. PRIOR EFFORTS TO OBTAIN EVIDENCE

25. Based upon my experience and training, it is not uncommon for technically sophisticated criminals to use encryption or programs to destroy data which can be triggered remotely or by a pre-programed event or keystroke, or other sophisticated techniques to hide data. In this case the data sought is stored on a server belonging to Dropbox. If data is accessed and deleted by the user, by either deleting the emails or any associated contact lists, the content would not be retrievable. Unlike traditional computer forensics where a hard drive can be searched and deleted documents recovered, information stored in an enterprise storage system is irretrievable once it has been deleted. Further, since this information is accessible from anywhere the suspect can obtain an Internet connection to log on to his account, he can delete this information in a matter of minutes.

26. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with the SUBJECT ACCOUNT owner, they could rightfully refuse to give consent and the SUBJECT ACCOUNT owner could arrange for destruction of all evidence of the crime before agents could obtain a search warrant.

Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT ACCOUNT. The suspect in this investigation has already demonstrated an ability to wipe computer hard drives to destroy evidence of child pornography.

V. PROTOCOL FOR SORTING SEIZABLE ELECTRONCALLY STORED INFORMATION

27. In order to ensure agents are limited in their search only to the contents of the SUBJECT ACCOUNT as described in Attachment B; in order to protect the privacy interests of other third parties who have accounts at Dropbox; and in order to minimize disruptions to normal business operations of Dropbox; this application seeks authorization to permit agents and employees of Dropbox to assist in the execution of the warrant, pursuant to 18 U.S.C. § 2703(g), as follows:

a. The search warrant will be presented to Dropbox, with direction that it identify and isolate the SUBJECT ACCOUNT and associated records described in Section I of Attachment B.

b. Dropbox will also be directed to create an exact duplicate in electronic form of the SUBJECT ACCOUNT and associated records specified in Section I of Attachment B, including an exact duplicate of the content of all email messages stored in the SUBJECT ACCOUNT.

c. Dropbox shall then provide an exact digital copy of the contents of the SUBJECT ACCOUNT, as well as all other records associated with the account, to me, or to any other agent of HSI. Once the digital copy has been received from Dropbox, that copy will, in turn, be forensically imaged and only that image will be reviewed and analyzed to identify communications and other data subject to seizure pursuant to Section II of Attachment B. The original digital copy will be sealed and maintained to establish authenticity, if necessary.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords search text, and many common electronic mail, database, and spreadsheet applications (which may be attached to email) do not store data as searchable text. The data is saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months.

e. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to seize all emails, chat logs and documents, which identify any users of the subject account and any emails sent or received in temporal proximity to incriminating emails which provide context to the incriminating communications.

f. All forensic analysis of the image data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

VI. CONCLUSION

28. Based upon the evidence gathered in this investigation as set out above, including but not limited to my review of data and records, information received from other law enforcement agents, and my training and experience, there is probable cause to believe evidence, fruits and/or instrumentalities of the crimes of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(Possession of Child Pornography) exists and will be found in the electronically stored information or communications contained and associated with the SUBJECT ACCOUNT and any attachments, stored instant messages, stored voice messages, documents, videos, and photographs associated therewith, as well as in subscriber and log records associated with the account. Accordingly, by this Affidavit and warrant I seek authority for the government to search all of the items specified in Attachment A and Section I of Attachment B (attached hereto and incorporated by reference herein) to the warrant, and specifically to seize all of the data, documents and records which are identified in Section II of Attachment B.

Dated this 21 day of November, 2016.

Toby Ledgerwood, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 21st day of November, 2016.

PAULA L. MCCANDLIS
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101
(206) 553-7970

ATTACHMENT A

Place to be Searched

All information associated with the Dropbox account "dblouin1966@gmail.com" stored at premises owned, maintained, controlled, or operated by Dropbox, a company headquartered at 185 Berry Street, Suite 400, San Francisco, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Section I - Items to be to be Provided by Dropbox Inc. for Search

1. All electronically stored information and communications contained in the Dropbox account, "dblouin1966@gmail.com" including associated email addresses; alternate email addresses; associated cloud storage; account registration information, user contact information, linked web addresses and posted images, content and logs; including a copy of these accounts.

2. All subscriber records associated with the specified accounts, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

3. Log records, including IP address captures, associated with the specified accounts;

4. Any address lists or buddy/contact lists associated with the specified account(s); and

5. Any records of communications between Dropbox Inc., and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified accounts. This is to include records of contacts between the subscribers and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Section II - Items to be Seized

From all electronically stored information and communications contained in the Dropbox account "dblouin@gmail.com" including associated email addresses; alternate email addresses; associated cloud storage accounts to include contents of electronic files:

a. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the accounts specified, or who exercise in any way any dominion or control over the specified accounts;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Any address lists or buddy/contact lists associated with the specified accounts;

c. All images of child pornography and any messages, documents and profile information, attachments, or other data related to child pornography or the possession, receipt, or distribution of child pornography;

d. All subscriber records associated with the specified accounts, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number(s);

e. Any and all other log records, including IP address captures, associated with the specified accounts; and

f. Any records of communications between Dropbox Inc. and any person about issues relating to the specified accounts, such as technical problems, billing inquiries, or complaints from other users about the specified accounts. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970